MICRO FOCUS

Open Enterprise Server 2018 SP3

Domain Services for Windows Security Guide

May 2021

Legal Notices

© Copyright 2017 - 2021 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Guide 5

1 Overview 7

2 Domain Services for Windows Security Model 9

2.1 DSfW Unit of Administration . . . 9
2.2 Partitions and Domains . . . 9
2.2.1 eDirectory Partitions . . . 10
2.2.2 DSfW Domains . . . 10
2.3 Understanding DSfW in Relation to Active Directory . . . 10
2.3.1 Additional Features of Active Directory . . . 11
2.4 DSfW Authentication . . . 11
2.5 Authenticating to Other Services . . . 12
2.6 SYSVOL Replication . . . 12

3 Using Access Control Lists in Domain Services for Windows 13

3.1 ACL Changes in a Tree When DSfW Is Installed . . . 13
3.1.1 Installing a New Domain . . . 13
3.1.2 Installing a Forest Root Domain . . . 16
3.1.3 Installing a Non-Name-Mapped Forest Root Domain . . . 16
3.1.4 Installing a Name-Mapped Forest Root Domain . . . 17

4 Trust Relationship of Domains in the Forest 19

5 Authentication Methods 21

5.1 Authentication Protocols . . . 21
5.1.1 LAN Manager . . . 21
5.1.2 NT LAN Manager (NTLM) . . . 21
5.1.3 Kerberos . . . 21
5.2 Authentication Methods . . . 22

6 Components of Domain Services for Windows 23

7 Using Group Policies to Secure Your Network 27

8 System Security Considerations 29

8.1 Firewalls . . . 29
8.1.1 DSfW Install Opens Ports 53 and 953 . . . 29
8.2 Starting and Stopping Services . . . 29
8.3 DNS . . . 30
8.4 Other Security Considerations . . . 30

9 General Security Considerations **31**

9.1 Disabling a Server from Being a Global Catalog Server 31
9.2 Retrieving Passwords. 31
9.3 Getting a UID Range for a Domain 31
9.4 Preventing Workstation Administrators from Accessing the SYSVOL Folder 32

10 Encryption **33**

11 Logging **35**

A Windows and Active Directory Terminology **37**

About This Guide

This guide describes security issues and recommendations for OES Domain Services for Windows for Open Enterprise Server 2018 SP3.

- Chapter 1, “Overview,” on page 7
- Chapter 2, “Domain Services for Windows Security Model,” on page 9
- Chapter 3, “Using Access Control Lists in Domain Services for Windows,” on page 13
- Chapter 4, “Trust Relationship of Domains in the Forest,” on page 19
- Chapter 5, “Authentication Methods,” on page 21
- Chapter 6, “Components of Domain Services for Windows,” on page 23
- Chapter 7, “Using Group Policies to Secure Your Network,” on page 27
- Chapter 8, “System Security Considerations,” on page 29
- Chapter 9, “General Security Considerations,” on page 31
- Chapter 10, “Encryption,” on page 33
- Chapter 11, “Logging,” on page 35
- Appendix A, “Windows and Active Directory Terminology,” on page 37

Audience

The guide is intended for security administrators or anyone who is responsible for the security of the system.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of this guide, see the OES 2018 SP3 documentation Web site (https://www.microfocus.com/documentation/open-enterprise-server/2018-SP3/).

Additional Documentation

For information on installing, configuring, and using OES Domain Services for Windows see *OES 2018 SP3: Domain Services for Windows Administration Guide*.

For eDirectory installation instructions, see the NetIQ eDirectory Installation Guide.

For documentation on the eDirectory management utility, see the NetIQ iManager Administration Guide.

For information on security vulnerabilities, see Security Considerations in the NetIQ eDirectory Administration Guide.

1 Overview

Domain Services for Windows (DSfW) is a suite of technologies that allows Microsoft Windows users to access OES services through native Windows and Active Directory protocols. By allowing OES servers to behave as if they were Active Directory servers, this technology enables companies with Active Directory and NetIQ eDirectory deployments to achieve better coexistence between the two platforms. Users can work in a pure Windows desktop environment and still take advantage of some OES back-end services and technology, without the need for a Client for Open Enterprise Server on the desktop.

Administrators can use either Micro Focus iManager or Microsoft Management Console (MMC) to administer users and groups. Network administrators manage file systems using the native tools of each server, and they can also centrally administer Samba shares on OES / DSfW servers by using iManager.

Administrators can use MMC to create one-way inter-domain trusts between DSFW domains and Active Directory domains.

When DSfW is deployed in an environment that also supports NetWare Core Protocol (NCP), DSfW supports cross-protocol locking. Whether customers decide to use only Windows clients, NCP clients, or a combination of both, access rights for files are enforced by the Storage Services (NSS) file system.

A DSfW server can be deployed without NSS. In these cases, the administrator runs Samba over a POSIX-compliant file system, but this loses the strong security provided by the OES rights and access models.

2 Domain Services for Windows Security Model

Domain Services for Windows (DSfW) emulates the Active Directory security model on top of eDirectory, so most of the security considerations for both Active Directory and eDirectory apply to DSfW. However, there are some key differences:

- Section 2.1, “DSfW Unit of Administration,” on page 9
- Section 2.2, “Partitions and Domains,” on page 9
- Section 2.3, “Understanding DSfW in Relation to Active Directory,” on page 10
- Section 2.4, “DSfW Authentication,” on page 11
- Section 2.5, “Authenticating to Other Services,” on page 12
- Section 2.6, “SYSVOL Replication,” on page 12

2.1 DSfW Unit of Administration

An organizational unit (OU) is the fundamental unit of administration in a DSfW environment/ directory structure. Administrative powers are commonly allotted at the OU level. Granular delegation can be performed on individual objects or attributes. An OU can contain other objects, including other OUs, which are also referred to as container objects. An OU can be nested to 10 levels to organize the directory and allow the creation of subdomains.

For efficient directory access, you can limit nesting to three or four levels. The OUs should be arranged to facilitate group policy application and administrative delegation. The Organizational Unit object usually represents a department, which holds a set of objects that commonly need access to each other.

A typical example is a set of users, along with the printers, volumes, and applications that those users need. At the highest level of Organizational Unit objects, each Organizational Unit can represent each site (separated by WAN links) in the network.

An OU forms an administrative boundary, and a tree forms the true security boundary.

For more information on the eDirectory structure, see Understanding NetIQ eDirectory in the NetIQ eDirectory Administration Guide.

2.2 Partitions and Domains

- Section 2.2.1, “eDirectory Partitions,” on page 10
- Section 2.2.2, “DSfW Domains,” on page 10

2.2.1 eDirectory Partitions

A partition in eDirectory is a logical group of objects in an eDirectory tree. Partitioning allows you to manage the tree by taking part of the directory from one server and putting it on another server. If you have slow or unreliable WAN links or if your directory has so many objects that the server is overwhelmed and access is slow, you should consider partitioning the directory.

Each directory partition consists of a set of container objects, all the objects contained in them, and data about those objects. eDirectory partitions don’t include any information about the file system or its directories and files. Partitions are named by their topmost container.

For a complete discussion of partitions, see Managing Partitions and Replicas in the NetIQ eDirectory Administration Guide.

2.2.2 DSfW Domains

A domain in DSfW is a security boundary that is similar to a partition in eDirectory. The domain also forms the administrative and security boundary for a logical group of network resources such as users or computers. Typically, a domain resides in a localized geographic location; however, this might not always be the case. Domains are commonly used to divide global areas of an organization and its functional units.

2.3 Understanding DSfW in Relation to Active Directory

eDirectory: eDirectory organizes objects in a tree structure, beginning with the top Tree object, which bears the tree's name. Whether your eDirectory servers are running Linux, UNIX, or Windows all resources can be kept in the same tree. You don’t need to access a specific server or domain to create objects, grant rights, change passwords, or manage applications. The hierarchical structure of the tree gives you great management flexibility and power. For more information on trees, see Understanding NetIQ eDirectory in the NetIQ eDirectory Administration Guide.

In eDirectory, the master replica is a writable replica type used to initiate changes to an object or partition The master replica is responsible for maintaining all replica and schema epochs. If a replication or schema problem needs to be corrected, the operation is performed from the master replica. If the directory has been partitioned into a number of replicas, a master replica is required on each server.

Active Directory: Active Directory is a hierarchical multilevel framework of objects. It provides information on the objects, organizes them, controls access to them and sets security. The logical divisions of an Active Directory network consist of forests, trees, and domains.

- **Domain:** In Active Directory, a domain is a security boundary that is similar to a partition in eDirectory. Each Active Directory domain that is configured to act as a Global Catalog stores a full copy of all Active Directory objects in the host domain and a partial copy of all objects for all other domains in the forest.
- **Forest:** A forest is a collection of Active Directory domains and is comparable to a tree in eDirectory
- **Trust Relationships:** You can set up trust relationships to share resources between domains. Federation can be accomplished through establishing cross-domain and cross-forest trusts.

- **Domain Names:** Active Directory uses domain class (DC) naming at the root of a naming context, as opposed to the X.500 naming used in eDirectory. For example, in eDirectory a partition is specified as ou=sales.o=company, but in Active Directory the partition is specified as dc=sales,dc=company,dc=com.
- **Security Model:** The Active Directory security model is based on shared secrets. The domain controller contains all users' keys. The authentication mechanism is based on Kerberos, NTLM, Smartcard, Digest etc.

The Active Directory security model is based on shared secrets. The domain controller contains all users' keys.

For more information on Active Directory forests, refer to the Active Directory Tutorial (http://searchwinit.techtarget.com/generic/0,295582,sid1_gci1050336,00.html)

2.3.1 Additional Features of Active Directory

- Within an Active Directory topology, distinct roles are defined, but these roles are not fixed. Any role can be moved to another server at any time. For more information about these roles, see "Flexible Single Master Operation (FSMO) Roles " in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.
- In Active Directory, Flexible Single Master Operation (FSMO) roles ensure directory integrity by policing specific operations that belong only on a single-server directory service. For example, FSMO roles enable Active Directory to avoid the simultaneous creation of new domains with identical names or the creation of concurrent schema extensions using the same attribute with a different underlying syntax.
- In Active Directory, the Primary Domain Controller Emulator FSMO role has two primary functions. It provides backward compatibility for Windows NT4 domains and for servers, and it acts as an accelerator for certain account management functions. For example, password changes and account lockouts are passed to the PDC Emulator FSMO role and then quickly replicated throughout a domain infrastructure.
- In a Microsoft environment, time synchronization is important primarily for maintaining Kerberos authentication. Time synchronization is not vital to the functioning of the primary domain controller.

2.4 DSfW Authentication

DSfW is both an authentication service and an application service to which you can authenticate by using previously acquired credentials.

For example, in a Windows logon session, the user acquires a Kerberos ticket granting ticket (TGT), and uses that ticket to acquire service tickets to log in to the local workstation and the DSfW LDAP server for group policy lookup. While performing network authentication to eDirectory through Kerberos, the user could just as well be authenticating to another service joined to the domain, for example, a file server.

DSfW abstracts network authentication by using the GSS-API. It uses NTLM and Kerberos, as well as a third pseudo-mechanism (SPNEGO) that can securely negotiate between arbitrary concrete mechanisms.

Initial (logon) authentication is provided by the KDC (for Kerberos) and the Net Logon service (for NTLM). Additionally, Net Logon also provides pass-through authentication for challenge response protocols such as NTLM and Digest (for Windows services).

2.5 Authenticating to Other Services

A product authenticates to eDirectory by using SASL EXTERNAL over IPC. It proves that it runs with the same POSIX identity and this is mapped to the domain controller account DN. The domain controller account is allowed to impersonate arbitrary users, so that it can operate with least privileges when performing operations on behalf of RPC clients.

2.6 SYSVOL Replication

SYSVOL replication is done over SSH tunnels using the Kerberos credentials of a proxy user that is set up and managed internally. The credentials are accessible only to the local root user.

3 Using Access Control Lists in Domain Services for Windows

In eDirectory and in Domain Services for Windows (DSfW), an access control list (ACL) is a list of permissions assigned to an object. The list specifies the access details of the object, and the operations that a user can perform on the object. A typical ACL entry specifies a subject and an operation.

For more information on ACLs in eDirectory, see eDirectory Rights in the NetIQ eDirectory Administration Guide.

3.1 ACL Changes in a Tree When DSfW Is Installed

ACL's are spanned across different LDIF files. The following sections describe in detail the ACL changes required for DSFW.

- Section 3.1.1, “Installing a New Domain,” on page 13
- Section 3.1.2, “Installing a Forest Root Domain,” on page 16
- Section 3.1.3, “Installing a Non-Name-Mapped Forest Root Domain,” on page 16
- Section 3.1.4, “Installing a Name-Mapped Forest Root Domain,” on page 17

3.1.1 Installing a New Domain

New domain: filename=nds-domain.ldif.

Object DN	Trustee DN	Attribute Name	Privileges
CN=Policies,CN=System,<DC=domain>	CN=Group Policy Creator Owners,CN=Users,<DC=domain>	All Attributes Rights	15
	CN=Group Policy Creator Owners,CN=Users,<DC=domain>	Entry Rights	15
DC=domain	CN=Administrator,CN=Users,<DC=domain>	dBCSPwd	4
	CN=Administrator,CN=Users,<DC=domain>	unicodePwd	4
	CN=Administrator,CN=Users,<DC=domain>	supplementalCredentials	4
	CN=Administrator,CN=Users,<DC=domain>	currentValue	4

Object DN	Trustee DN	Attribute Name	Privileges
	CN=Administrator,CN=Users,<DC=domain>	priorValue	4
	CN=Administrator,CN=Users,<DC=domain>	initialAuth Incoming	4
	CN=Administrator,CN=Users,<DC=domain>	initialAuth Outgoing	4
	CN=Administrator,CN=Users,<DC=domain>	trustAuthIncoming	4
	CN=Administrator,CN=Users,<DC=domain>	trustAuthOutgoing	4
	CN=Domain Admins,CN=Users,<DC=domain>	dBCSPwd	4
	CN=Domain Admins,CN=Users,<DC=domain>	unicodePwd	4
	CN=Domain Admins,CN=Users,<DC=domain>	supplementalCredentials	4
	CN=Domain Admins,CN=Users,<DC=domain>	currentValue	4
	CN=Domain Admins,CN=Users,<DC=domain>	priorValue	4
	CN=Domain Admins,CN=Users,<DC=domain>	initialAuth Incoming	4
	CN=Domain Admins,CN=Users,<DC=domain>	initialAuth Outgoing	4
	CN=Domain Admins,CN=Users,<DC=domain>	trustAuthIncoming	6
	CN=Domain Admins,CN=Users,<DC=domain>	trustAuthOutgoing	6
	CN=Administrators,CN=Builtin,<DC=domain>	All Attributes Rights	32
	CN=Administrators,CN=Builtin,<DC=domain>	Entry Rights	16

Object DN	Trustee DN	Attribute Name	Privileges
	CN=Domain Admins,CN=Users,<DC=domain>	All Attributes Rights	15
	CN=Domain Admins,CN=Users,<DC=domain>	Entry Rights	15
	CN=Group Policy Creator Owners,CN=Users,<DC=domain>	gPLink	7
	CN=Group Policy Creator Owners,CN=Users,<DC=domain>	gPOptions	7
	CN=Cert Publishers,CN=Users,<DC=domain>	userCertificate	7
	OU=Domain Controllers,<DC=domain>	All Attributes Rights	32
	CN=Domain Controllers,CN=Users,<DC=domain>	All Attributes Rights	32
	OU=Domain Controllers,<DC=domain>	Entry Rights	16
	CN=Domain Controllers,CN=Users,<DC=domain>	Entry Rights	16
	CN=Domain Computers,CN=Users,<DC=domain>	PasswordExpirationInterval	3
	CN=Domain Computers,CN=Users,<DC=domain>	PasswordMinimumLength	3
	CN=Domain Computers,CN=Users,<DC=domain>	nspmConfigurationOptions	3
	CN=Domain Computers,CN=Users,<DC=domain>	nspmMinPasswordLifetime	3
	CN=Domain Computers,CN=Users,<DC=domain>	pwdInHistory	3
CN=Configuration,<DC=domain>	CN=Administrator,CN=Users,<DC=domain>	All Attributes Rights	32

Object DN	Trustee DN	Attribute Name	Privileges
	CN=Administrator,CN=Users,<DC=domain>	Entry Rights	16

3.1.2 Installing a Forest Root Domain

Forest root domain: filename=nds-admin-acls.ldif

Object DN	Trustee DN	Attribute Name	Privileges
<DC=domain>	CN=Enterprise Admins,CN=Users,<DC=domain>	All Attributes Rights	32
	CN=Enterprise Admins,CN=Users,<DC=domain>	Entry Rights	16
CN=Configuration,<DC=domain>	CN=Enterprise Admins,CN=Users,<DC=domain>	All Attributes Rights	32
	CN=Enterprise Admins,CN=Users,<DC=domain>	Entry Rights	16
CN=Schema,CN=Configuration,<DC=domain>	CN=Schema Admins,CN=Users,<DC=domain>	All Attributes Rights	32
	CN=Schema Admins,CN=Users,<DC=domain>	Entry Rights	16

nds-domain-acls.ldif

Object DN	Trustee DN	Attribute Name	Privileges
<DC=domain>	Public	cn	1
	This	dBCSPwd	4
	This	unicodePwd	4
	This	supplementalCredentials	4

3.1.3 Installing a Non-Name-Mapped Forest Root Domain

Non-name mapped forest root domain: filename=nds-domain-lum-acls.ldif.

Object DN	Trustee DN	Attribute Name	Privileges
<DC=domain>	Public	gecos	2
	Public	gidNumber	2
	Public	uidNumber	2
	Public	unixHomeDirectory	2
	Public	loginShell	2
	Public	memberUid	2

nds-super-rights-acls.ldif

Object DN	Trustee DN	Attribute Name	Privileges
Root server object	CN=<hostname>,OU=Domain Controllers,<DC=domain>	Entry Rights	16
	CN=<hostname>,OU=Domain Controllers,<DC=domain>	All Attributes Rights	32

3.1.4 Installing a Name-Mapped Forest Root Domain

Name-mapped forest root domain: filename=nds-domain-rights-acls.ldif

Object DN	Trustee DN	Attribute Name	Privileges
<DC=domain>	CN=<hostname>,OU=Domain Controllers,<DC=domain>	Entry Rights	16
	CN=<hostname>,OU=Domain Controllers,<DC=domain>	[All Attributes Rights	32

4 Trust Relationship of Domains in the Forest

A trust is used to allow users of one domain to access resources from another domain. Trusts are automatically created within an eDirectory tree when domains are created. For authentication and name lookups to work across domains, a trust relationship must be created between the domains. The trust relationship includes a shared secret that can be used for both Kerberos and NTLM authentication, along with information that is used to support name resolution.

Domains can have trust relationships to other domains, which permit a user in one domain to be authenticated to another. These relationships are manifested as shared secrets between the two domains. Trust relationships are automatic (and transitive) within a forest; they can also be explicitly created to external domains or forests.

For more details about the kinds of trusts and setting up trusts, see "Managing Trust Relationships in Domain Services for Windows" in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.

5 Authentication Methods

This section explains the authentication methods available for Domain Services for Windows (DSfW) and also provides details on what authentication mechanisms are used for different connections.

Kerberos is the principal authentication mechanism for eDirectory and DSfW. However, earlier authentication protocols are also maintained for backward compatibility.

- Section 5.1, “Authentication Protocols,” on page 21
- Section 5.2, “Authentication Methods,” on page 22

5.1 Authentication Protocols

- Section 5.1.1, “LAN Manager,” on page 21
- Section 5.1.2, “NT LAN Manager (NTLM),” on page 21
- Section 5.1.3, “Kerberos,” on page 21

5.1.1 LAN Manager

LAN Manager uses a two-part, 32-bit password hash. The first seven bits make up the first part of the hash; the last seven characters make up the second part of the hash (thus, the 14-character maximum password size). Consequently, if you have a seven-character password, the second 16 characters of the password hash are the same as the first 16 characters, revealing to an attacker that the password is only seven characters.

5.1.2 NT LAN Manager (NTLM)

This is a more secure challenge-response authentication protocol than LAN Manager. It uses 56-bit encryption for protocol security and stores passwords as an NT hash. Windows NT 4.0 Service Pack 3 (SP3) and earlier clients use this protocol.

NTLMv2 uses 128-bit encryption and is used for machines running NT 4.0 SP4 and later. This is the most secure challenge-response authentication available.

5.1.3 Kerberos

Kerberos is a trusted third-party authentication system. based on the Needham-Schroeder model. For more information refer, section 1.1 of RFC 4120 for a description of the terms principal, Authentication Service (AS), Ticket Granting Service (TGS), Ticket Granting Ticket (TGT), service ticket (STKT).

5.2 Authentication Methods

This section provides details on the various authentication mechanisms used for validating the connections that happen over different protocol or ports. DSfW authenticates in different ways, depending on the type of authentication and the protocols and ports that are used.

- **Login:** When the user logs in, network authentication happens through Kerberos or NTLM .
- **LDAP over TCP:** LDAP communication over the TCP protocol happens through Kerberos or NTLM with the help of the Simple Authentication and Security Layer (SASL) framework for authentication and data security.
- **LDAP over IPC:** In case of LDAP communication over the IPC protocol, authentication and authorization are based on the process identity represented by the effective UID. The local root user is granted full access and can assume the identity of other directory users using SASL-IPC External mechanism.
- **SMB:** Authentication with SMB happens through Kerberos or NTLM.
- **RPC:** Authentication with RPC happens through Kerberos or NTLM.
- **RPC portmapper:** No authentication is required for communicating with the RPC portmapper server.
- **DNS:** When a workstation is joined to the domain, the authentication happens through Kerberos. No authentication is required for a DNS lookup.
- **NTP:** Authentication to NTP happens through the MD5 encryption algorithm.
- **rsynch over SSH:** Authentication for rsynch data transmission over an SSH channel happens through Kerberos. The SSH channel connection is established by using the identity of the domain controller.

6 Components of Domain Services for Windows

This section describes the various components and subcomponents of Domain Services for Windows (DSfW).

Table 6-1 *Components of DSfW*

Component	Subcomponent
eDirectory 9.2.1	
NMAS 3.3.4	
MIT Kerberos 1.6.2	
KDC and libraries: Includes the Kerberos authentication service and ticket granting service components.	
GSS-API: The framework for selecting and negotiating between multiple security mechanisms (For DSfW, they are SPNEGO, NTLM, and Kerberos).	
XAD framework: Implements the Active Directory information and security models, and contains a variety of plug-ins for eDirectory, NMAS, and MIT Kerberos	The Active Directory Provisioning Handler (ADPH) that enforces the Security Accounts Manager inside the DSA.
	The GSS and IPC SASL mechanisms (with associated LCM/LSMs), that provide GSS-API and UNIX authentication security to directory clients. The GSS mechanism also provides confidentiality and integrity services for NLDAP.
	The GSS and Net Logon DCE authentication mechanisms.
	The NTLMv2 authentication protocol (implemented as a GSS mechanism).
	The dcinit suite of domain controller provisioning scripts.
	A MIT Kerberos KDC back end that retrieves principal information for the Active Directory information model
SLAPI Plug-ins	nad: Active Directory information model for NLDAP.
	subschema: – Schema cache and subschema introspection.

Component	Subcomponent
	crossref: Used for generation of referrals and search result references, and Active Directory search semantics.
	addrdnvalues: Adds RDN values on entry.
	anr: Used for ambiguous name resolution.
	tokengroups: Generates a list of SIDs of user's group memberships.
	netlogon: Service used by Windows clients to locate domain controllers.
	rootdse: Additional attributes on root DSEs.
	ntacl: Support for Windows security descriptors.
	whoami: RFC 4532 (determines authorization identity for a connection).
	sam (pre-ADPH): Implements Active Directory SAM constraints.
	rfc2307 (pre-ADPH): Sets default RFC 2307 attributes for users.
	idmap_ad: Maps between SIDs and RFC 2307 UIDs/ GIDs.
	dce_funnel: Forwards CIFS encapsulated RPCs to xadsd.
	auth_paula: Forwards NTLM authentication requests to xadsd.
	netlogon: Forwards NMB locator requests to LDAP.
RPC Systems	Local Security Authority (LSARPC): SID to name translation, establishment of trusted domains, inter alia.
	Security Accounts Manager remote protocol (SAMR): SID-to-name translation, account management.
	Net Logon: Manages the secure channel between workstations and domain controllers, which is used for pass-through authentication, listing trusted domains, updating machine account shared secrets, etc.
	Directory Replication Service User API (DRSUAPI): Used for directory-based name translation and for replication with Active Directory servers replication is not supported by DSfW 1.0).

Component	Subcomponent
	Private Authentication Layer (PAULA): Used by Samba on DSfW domain controllers to forward NTLM authentication requests. Directory Services Setup (DSSetup): Information about the state of the domain controller.
SAMBA: Used for serving group policy information and forwarding RPCs encapsulated in the CIFS protocol to XAD). NTP with Net Logon extensions: Used for securely synchronizing network time, which is necessary for the Kerberos protocol. Novell BIND with GSS extensions: Used for securely updating workstation address information in DNS. DNS records are maintained in eDirectory. System Volume (SYSVOL): Contains the file system group policies (known as Group Policy Templates or GPT). The policies are replicated between domain controllers of the same domain by using the rsync utility.	

Apart from static configuration information, all of the component information is stored in eDirectory. Some information is managed by the directory server itself, including attributes whose integrity is critical to the Windows security model (for example, security identifiers, which can only be allocated by a trusted entity such as the directory server itself).

Most information is managed over LDAP and RPC by using the MMC management tools that ship with Windows.

7 Using Group Policies to Secure Your Network

Domain Services for Windows (DSfW) supports all Group Policy settings that apply to Windows servers and workstations. Group Policy settings that apply to domain controllers (such as Password policies) are not supported in the OES 2018 and later environment. The Password policies for DSfW users are controlled by eDirectory and the Universal Password settings.

For more information see, "Managing Group Policy and Fine-Grained Password Policy Settings" in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.

8 System Security Considerations

This chapter contains the following topics:

- Section 8.1, “Firewalls,” on page 29
- Section 8.2, “Starting and Stopping Services,” on page 29
- Section 8.3, “DNS,” on page 30
- Section 8.4, “Other Security Considerations,” on page 30

8.1 Firewalls

- Section 8.1.1, “DSfW Install Opens Ports 53 and 953,” on page 29

8.1.1 DSfW Install Opens Ports 53 and 953

If OES DNS is installed separately, YaST opens ports 53 and 953 in the firewall.

For more information about ports, see “Network Ports Used by DSfW ” in the *OES 2018 SP3: Domain Services for Windows Administration Guide*

8.2 Starting and Stopping Services

There are a number of components that must be restarted in a specific order. Use the `xadcntrl reload` command to reload them. This command will stop and start the services in the specific order.

1. ndsd (eDirectory)
2. novell-named (DNS)
3. nscd (name server cache daemon)
4. rpcd (RPC server)
5. Xad-krb5kdc (Kerberos)
6. xad-kpasswdd (Kpassword)
7. xadsd (XAD daemon)
8. nmb (NMB server, NETBIOS lookup)
9. winbind (winbind)
10. smb (Samba)
11. sshd (SSH)
12. rsyncd (rsync)

8.3 DNS

DSfW uses the OES DNS service as its location service, enabling users or computers to find the location of network resources. DNS maps hostnames to IP addresses and locates the services provided by the domain, such as LDAP, Kerberos and Global Catalog.

For more information on working of DNS with DSfW, see "Understanding DNS in Relation to DSfW" in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.

8.4 Other Security Considerations

- If a request comes over LDAPI and the mechanism used is external, then passwords can be retrieved provided the requests come from the local root user. This access is audited by eDirectory, and can be monitored for misuse.
- To disable the Global Catalog search on a particular server, ensure that the LDAP server is not configured for ports 3268 or 3269.

  Although this disables Global Catalog search, it also impacts the functioning of the DSfW server.
- If you use a name-mapped installation, you are installing DSfW in an existing tree. To ensure that the installation does not encounter errors, make sure you meet the prerequisites documented in Installation Prerequisites for a Name-Mapped Setup in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.
- When a computer account in the DSfW domain is created with password, the key version number attribute is by default set to 1 and is incremented by 1 each time the password is changed for this account.
- The gidNumber attribute used by LUM and the primaryGroupID attribute used by Samba refer to the same object.
- DSfW requires some DNS objects for smooth operation of the location service. For more details, see "General DNS Settings" in the *OES 2018 SP3: Domain Services for Windows Administration Guide*.
- When the DSfW server is provisioned, secure dynamic updates are enabled as part of the Update Service Configuration task. Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

9 General Security Considerations

- Section 9.1, “Disabling a Server from Being a Global Catalog Server,” on page 31
- Section 9.2, “Retrieving Passwords,” on page 31
- Section 9.3, “Getting a UID Range for a Domain,” on page 31
- Section 9.4, “Preventing Workstation Administrators from Accessing the SYSVOL Folder,” on page 32

9.1 Disabling a Server from Being a Global Catalog Server

To disable the Global Catalog search on a particular server, you must ensure that the LDAP server is not configured for ports 3268 or 3269. To disable global catalog search, follow the steps given below:

1. Log in to iManager and click **LDAP > LDAP options**.
2. Click the **View LDAP Servers** tab.
3. Click the server for which you want to disable global catalog search.
4. Click the **Connections** tab and edit the **LDAP Interfaces** field to remove the LDAP URL for ports 3268 and 3269.

Although this disables the Global Catalog search, it also impacts the functioning of the DSfW server. For example, by disabling Global Catalog search, operations such as searching of information in a DSfW forest will not work.

9.2 Retrieving Passwords

If a request comes over LDAPI and the mechanism used is external, passwords can be retrieved if the requests come from the root user.

9.3 Getting a UID Range for a Domain

You can check the domain UID range of a Domain Services for Windows (DSfW) server for the current domain by using the following command:

```
/opt/novell/xad/share/dcinit/provisionTools.sh get-uid-range
```

9.4 Preventing Workstation Administrators from Accessing the SYSVOL Folder

When a workstation accesses a domain, if the local administrator password is same as the domain administrator's password, the user can access the SYSVOL folder.

To prevent this, change the Security policy on the workstation by setting the LAN Manager authentication level to NTLMv2 instead of the default level of NTLMv1. For more information on security settings and editing security settings, refer to Network security: LAN Manager authentication level (http://technet.microsoft.com/en-us/library/cc738867%28WS.10%29.aspx).

10 Encryption

- **LDAP over TCP:** LDAP communication over the TCP protocol is encrypted GSS-API mechanism.
- **CLDAP:** CLDAP communication is not encrypted.
- **Kerberos:** All Kerberos packets are encrypted and protected by NICI SDI key in eDirectory.

  Kerberos keys in file (required by Samba and xadsd) are not encrypted.
- **File access over SMB:** Any file access through SMB is not encrypted.
- **RPC (over SMB or TCP):** Any remote procedure calls through SMB or TCP mostly encrypted.
- **DNS:** Name resolution queries are not encrypted. But dynamic updates are secured by TSIG key encryption.
- **File Replication:** Changes to file are replicated to domain controllers using rsynch method via SSH channel.

The NTLM keys are obfuscated with the user's relative identifier (RID) and stored in eDirectory.

11 Logging

Different log files are used to capture logging details of services and utilities.

Table 11-1 *Log Details*

Service	Log File
DNS	Details are logged in the `/var/opt/novell/log/named/named.run` file.
NTP	Details are logged in the `/var/log/ntp` file.
SSH	Details are logged in the `/var/log/messages` file.
rsync	Details are logged in the `/var/log/messages` file.
xadsd	Details are logged in the `/var/log/messages` file. Only critical events are logged.
sysvolsync	Details are logged in the `/var/opt/novell/xad/log/sysvolsync.log` file.
Kerberos	Details are logged in the `/var/opt/novell/xad/log/kdc.log` file.
Samba	Details are logged in the `/var/log/samba/log.smbd` file.
eDirectory startup	Details are logged in the `/var/opt/novell/eDirectory/log/ndsd.log` file.
eDirectory running	Details are logged in the `/var/opt/novell/eDirectory/log/ndstrace.log` file.
Winbindd parent process	Details are logged in the `/var/log/samba/log.winbindd` file.
Winbindd Interaction	Details are logged in `/var/log/samba/log.wb-<DOMAIN>` file.
Winbindd id-mapping	Details are logged in the `/var/log/samba/log.winbindd-idmap` file.

LDAP events are not logged by eDirectory.

In addition to these log files, the Provisioning Wizard also records the details and status of events happening in the background during the execution of each task. For more details, see “Logging” in the *OES 2018 SP3: Domain Services for Windows Administration Guide*

A Windows and Active Directory Terminology

- **User Principal Name (UPN):** An alias for a Kerberos user principal that can be used at logon time instead of the canonical Kerberos principal name.
- **Service Principal Name (SPN):** A Kerberos principal that is used by a service.Multiple SPNs can be associated with a single service object in the directory, to account for offering multiple services and naming differences (such as unqualified and qualified host names, or DNS and NetBIOS domain names).
- **Security Principal:** An entity that can be used as an authorization subject and can be an authentication subject for users. In the Windows security model, security principals are identified by a string known as a Security Identifier, or SID.
- **SID:** A unique alphanumeric character string that is assigned during the logon process. A SID is used to identify a subject, such as a user or a group of users. A SID is hierarchical and consists of a component that represents the authority that issued it (usually a domain) and a relative identifier.
- **Domain:** In Active Directory, a subdivision within a tree. An Active Directory domain is both a security boundary and a directory (partition) boundary.
- **Tree:** A set of hierarchically joint domains that are (transitively) trusted.
- **Forest:** In Active Directory forest, a set of possibly disjoint trees that are (transitively) trusted and share a global catalog and schema.
- **Global Catalog:** In an Active Directory Global Catalog, a sparse replica of all domains in a forest.
- **Services:** Services are first-class security principals (users) in Active Directory.
- **Authentication:** The process by which a computer validates a user's logon information. Active Directory supports two forms of trusted third-party authentication: Kerberos (Needham-Schroeder model) and NTLM/Digest (challenge-response model).